Defense Message System (DMS)

The Defense Message System (DMS) is designed to enable anyone in DoD to exchange both classified and unclassified messages with anyone else in DoD using a secure, accountable, and reliable writer-to-reader messaging system. DMS supports organizational and individual messaging, although only organizational messaging provides the ability to sign and encrypt messages using Fortezza cards. DMS is intended to reduce the cost and manpower demands of the legacy Automatic Digital Network (AUTODIN) organizational messaging system. To replace AUTODIN, DMS must be implemented in more than 40,000 organizations at more than 700 sites worldwide and must support message exchanges with tactical forces, allies, other Federal Government users, and defense contractors. The DMS program will ensure innovation by employing the latest commercial technology, supporting Allied Communications Publications 120, and operating on Defense Information Infrastructure computers and communications backbone. While today's security needs require using the international X.400 messaging standard and X.500 directory services standard, the DMS program expects to eventually move to the use of commercial Internet e-mail standards once they evolve to adequately support security and military features. The timeline for such evolution is unclear at this time, but is a number of years in the future.

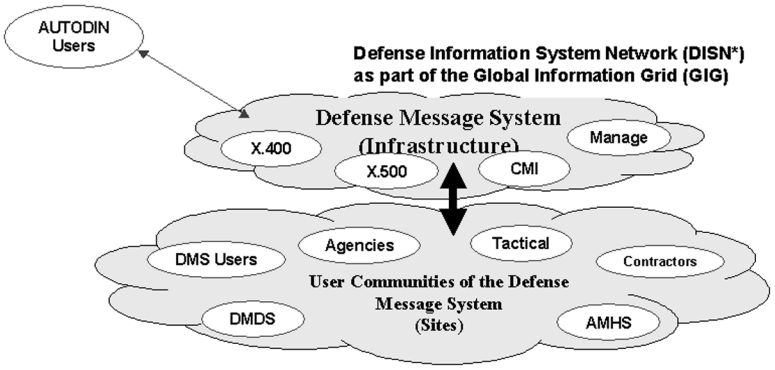
The Defense Information Systems Agency started the DMS program in 1988. Since the 1997 Initial Operational Test and Evaluation of release 1.0, DMS has continued to improve through operational assessments (OAs) in 1998 and 1999, and operational tests and evaluations (OT&Es) of releases 2.1 and 2.2. The AUTODIN backbone has been downsized to three message-switching centers called DMS Transition Hubs. Most tests have revealed difficulties with site installations, configurations, and overall security posture of DMS. DMS 2.2 Gold was approved for fielding in 2001, and DMS 3.0 was approved for fielding to the General Services (GENSER) and tactical communities in May 2002.

TEST & EVALUATION ACTIVITY

- DMS 3.0 OT&E, late Spring 2002, for the GENSER and Air Force tactical communities.
- DMS 3.0 OA for the Intelligence Community (IC), conducted in conjunction with the GENSER community OT&E. The IC plans to conduct an OT&E of the IC solution in Spring 2003.
- Operational assessment of the Army's Tactical Messaging System during the Joint User Interoperability Communications Exercise (JUICE) 2002 communications exercise in August 2002.

TEST & EVALUATION ASSESSMENT

DMS 3.0 performed well for the GENSER and Air Force tactical communities during OT&E. However, with respect to the Critical Operational Issue (COI) on security, tests revealed that system administrators had again failed to protect all elements, primarily attributable to poor security password practices at many of the sites. This COI was unfavorably resolved. The operational test agency, Joint Interoperability Test Command (JITC), found that other than poor password practices, DMS did not have other significant vulnerabilities, and therefore determined the system to be operationally suitable. Administering DMS requires attention to detail and relies heavily on complex documentation and manual configuration. System administrators were very competent in administering the system, although in



The Defense Message System is designed to enable anyone in DoD to exchange both classified and unclassified messages with anyone else in DoD using a secure, accountable, and reliable writer-to-reader messaging system. DMS supports organizational and individual messaging.

general they required assistance from the developer to initially configure the system. The Program Management Office must continue to streamline system operations and system administration tasks, improve training, and enhance documentation. The system administrators must strictly follow all established security policies and procedures. There are several significant operational concerns with DMS. Two of these address the complexity of the DMS Certificate Management Infrastructure (CMI) and the risk associated with value added products not going through the JITC developmental test process.

Although many measures of effectiveness were successfully met, the IC's OA of DMS 3.0 showed that the IC solution was not sufficiently mature for a full OT&E. Interfacing to the legacy AUTODIN system was problematic within the IC. There were also problems with certificates and Fortezza cards within the CMI.

During the JUICE 2002 exercise, the test of the Army Tactical Messaging System showed that the system hardware and the DMS software worked very well. However, system administrators again experienced difficulties with Fortezza cards, initial configuration of the system, and interfacing with the legacy AUTODIN.